Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for authorizing a client to access a service based on compliance with a policy required for access to the service, the method comprising:
specifying a policy required for access to the service;
detecting a request for access to the service from a client;
attempting authentication of the client based on credentials presented by the client;
if the client is authenticated based on the credentials, determining whether the client is in compliance with said policy based, at least in part, on attributes of the client; and
if the client is determined to be in compliance with said policy, providing access to the service.

[c2] 2. The method of claim 1, wherein the service comprises a remote service accessible by the client through a network.

[c3] 3. The method of claim 1, further comprising:
restricting access to the service if the client is determined to be non-compliant with said policy.

[c4] 4. The method of claim 3, wherein restricting access includes assigning limited access privileges to the client.

[c5] 5. The method of claim 3, wherein restricting access includes issuing a Kerberos ticket specifying limited access privileges if the client is determined to be non-compliant with the policy.

[c6] 6. The method of claim 1, wherein said policy comprises a security policy.

[c7] 7. The method of claim 6, wherein said security policy includes security measures required on the client.

[c8] 8. The method of claim 1, wherein said policy includes anti-virus measures required on the client.

[c9] 9. The method of claim 1, wherein said step of providing access includes issuing a Kerberos ticket specifying access privileges provided to the client.

[c10] 10. The method of claim 1, wherein attributes of the client include a selected one of a file integrity policy in effect at the client, a file installed at the client, a process running at the client, a particular checksum value at the client, and a registry entry at the client.

[c11] 11. The method of claim 1, wherein said detecting step includes detecting a request for access to a server by a

remote client.

[c12] 12. The method of claim 1, wherein said detecting step includes detecting a request for access to a service on a computer system by another process on the computer system.

[c13] 13. The method of claim 1, wherein said attempting authentication step includes authentication based on user identity.

[c14] 14. The method of claim 1, wherein said attempting authentication step includes using a selected one of Kerberos authentication, Pluggable Authentication Module (PAM) authentication, Extensible Authentication Protocol (EAP) authentication, Generic Security Service API (GSS-API) authentication, and trust negotiation in TLS (TNT) authentication.

[c15] 15. The method of claim 1, wherein said credentials include a selected one of a user name, a password, and a certificate.

[c16] 16. The method of claim 1, wherein said determining step includes obtaining attribute information from the client.

[c17] 17. The method of claim 16, wherein said step of ob-

taining information from the client includes requesting attribute information collected by a client-side component.

[c18] 18. The method of claim 1, wherein said determining step includes substeps of:
providing a copy of the policy to the client; and
performing a compliance check at the client to determine compliance with the policy.

[c19] 19. The method of claim 1, wherein said determining step includes obtaining information from a security evaluation service that has previously evaluated compliance by the client with the policy.

[c20] 20. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

[c21] 21. A downloadable set of processor-executable instructions for performing the method of claim 1.

[c22] 22. A system for authenticating and assigning access privileges to a client device for access to a service, the system comprising:
a policy specifying access privileges to be assigned to a client device based on attributes of the client device;
a primary authentication module for receiving a request

from a client device for access to the service and determining whether to authenticate the client device for access to the service; and

a supplemental authentication module for examining attributes of a client device authenticated by said primary authentication module and assigning access privileges to the client device based on the policy.

[c23] 23. The system of claim 22, wherein said policy comprises a security policy.

[c24] 24. The system of claim 22, wherein said policy includes security attributes of the client device.

[c25] 25. The system of claim 22, wherein said step of examining attributes of the client device includes determining whether specified anti-virus measures are in effect on the client device.

[c26] 26. The system of claim 22, wherein said step of examining attributes of the client device includes examining a selected one of a file integrity policy in effect at the client device, a file installed at the client device, a process running at the client device, a particular checksum value at the client device, and a registry entry at the client device.

[c27] 27. The system of claim 22, wherein said primary au-

thentication module uses a selected one of Kerberos authentication, Pluggable Authentication Module (PAM) authentication, Extensible Authentication Protocol (EAP) authentication, Generic Security Service API (GSS-API) authentication, and trust negotiation in TLS (TNT) authentication.

[c28] 28. The system of claim 22, wherein said primary authentication module authenticates the client device based upon user identity.

[c29] 29. The system of claim 28, wherein the client device provides a user name and password to said primary authentication module for authenticating user identity.

[c30] 30. The system of claim 28, wherein the client device provides a digital certificate to said primary authentication module for authenticating user identity.

[c31] 31. The system of claim 22, wherein the supplemental authentication module includes a component on the client device for collecting attribute information.

[c32] 32. The system of claim 31, wherein the component on the client device evaluates the collected attribute information at the client device for determining compliance of the client device with the policy.

[c33] 33. The system of claim 32, further comprising:
a policy server for providing the policy to the client device.

[c34] 34. The system of claim 22, wherein the supplemental authentication module receives information about attributes of the client device from the client device.

[c35] 35. The system of claim 34, wherein the client device provides attribute information to the supplemental authentication module in response to a message from the supplemental authentication module.

[c36] 36. The system of claim 35, wherein said attribute information is provided as a selected one of a text string, an Extensible Markup Language (XML) document, and an Abstract Syntax Notation One (ASN.1) file.

[c37] 37. The system of claim 22, wherein the supplemental authentication module permits access to the service if the client device is in compliance with the policy.

[c38] 38. The system of claim 22, wherein the supplemental authentication module issues a Kerberos ticket specifying the client device's access privileges.

[c39] 39. The system of claim 22, wherein the supplemental authentication module restricts access to the service if

the client device is non-compliant with the policy.

[c40] 40. The system of claim 22, further comprising:
a policy server in communication with the supplemental authentication module for evaluating compliance by the client device with the policy based upon attributes of the client device.

[c41] 41. The system of claim 22, wherein the supplemental authentication module comprises a selected one of an anti-virus engine, a configuration checker, and a security engine.

[c42] 42. A method for assigning privileges to a client to use a service based on an access policy, the method comprising:
specifying an access policy for assigning privileges to a client to use the service based on attributes of the client;
detecting a request for use of the service from a client;
attempting authentication of the client based on user identity information provided by the client;
if the client is authenticated based on user identity, collecting attribute information from the client; and
assigning privileges to the client to use the service based on the collected attribute information and the access policy.

[c43] 43. The method of claim 42, wherein said step of assigning privileges includes blocking access to the service if the client is determined to be non-compliant with the access policy.

[c44] 44. The method of claim 42, wherein said step of assigning privileges includes restricting access to the service if the client is determined to be non-compliant with the access policy.

[c45] 45. The method of claim 42, wherein set step of assigning privileges includes issuing a Kerberos ticket to the client.

[c46] 46. The method of claim 42, wherein said access policy includes security measures required on the client.

[c47] 47. The method of claim 42, wherein said access policy includes anti-virus measures required on the client.

[c48] 48. The method of claim 42, wherein said access policy includes an attribute required for the client.

[c49] 49. The method of claim 48, wherein said attribute includes a selected one of a file integrity policy in effect at the client, a file installed at the client, a process running at the client, a particular checksum value at the client, and a registry entry at the client.

[c50] 50. The method of claim 42, wherein said detecting step includes detecting a request for access to a server by a remote client.

[c51] 51. The method of claim 42, wherein said collecting step includes requesting attribute information from the client.

[c52] 52. The method of claim 51, wherein the attribute information is provided as a selected one of a text string, an Extensible Markup Language (XML) document, and an Abstract Syntax Notation One (ASN.1) file.

[c53] 53. The method of claim 42, wherein said collecting step includes using a client-side component for collecting attribute information.

[c54] 54. The method of claim 53, wherein said client-side component determines whether the client is in compliance with the access policy based on the collected attribute information.

[c55] 55. The method of claim 53, wherein said client-side component sends the collected attribute information to a policy server for determining whether the client is in compliance with the access policy.

[c56] 56. A computer-readable medium having processor-executable instructions for performing the method of

claim 42.

[c57] 57. A downloadable set of processor-executable instructions for performing the method of claim 42.

[c58] 58. In a system comprising a client computer connecting to a service through a network, a method for regulating access to the service based on a specified access policy, the method comprising:
transmitting a challenge from the service to the client computer connecting to the service for determining whether the client computer is in compliance with said specified access policy, wherein said access policy includes attributes of the client device that are acceptable for permitting access to the service;
transmitting a response from the client computer back to the service, for responding to the challenge issued by the service; and
blocking access to the service by the client computer if the client computer does not respond appropriately to the challenge issued by the service.

[c59] 59. The method of claim 58, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

[c60] 60. The method of claim 58, wherein said challenge in-

cludes at least some rules of said access policy that are transmitted to the client computer.

[c61] 61. The method of claim 58, wherein said access policy is provided at the client computer.

[c62] 62. The method of claim 61, wherein the client computer performs a compliance check for determining compliance with the access policy and returns the compliance check result in response to the challenge.

[c63] 63. The method of claim 58, wherein said attributes include a selected one of a file integrity policy in effect at the client computer, a file installed at the client computer, a process running at the client computer, a particular checksum value at the client computer, and a registry entry at the client computer.

[c64] 64. The method of claim 58, further comprising: otherwise, permitting access to the service by the client computer.

[c65] 65. The method of claim 64, wherein permitting the client computer to access the service includes assigning access privileges based on the response received from the client computer.

[c66] 66. The method of claim 65, wherein assigning access

privileges includes issuing a Kerberos ticket for providing said access privileges to the client computer.

[c67] 67. A downloadable set of processor-executable instructions for performing the method of claim 58.

[c68] 68. A computer-readable medium having processor-executable instructions for performing the method of claim 58.